(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 404 041**

(51) Int. CI.:

H04N 21/266 (2011.01)
H04N 21/4623 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.11.2005 E 05851894 (5)**

(97) Fecha y número de publicación de la concesión europea: **20.03.2013 EP 1815682**

(54) Título: **Sistema y método para proporcionar acceso autorizado a contenido digital**

(30) Prioridad:

17.11.2004 US 628786 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.05.2013

(73) Titular/es:

GENERAL INSTRUMENT CORPORATION (100.0%)
101 TOURNAMENT DRIVE
HORSHAM, PENNSYLVANIA 19044, US

(72) Inventor/es:

MEDVINSKY, ALEXANDER

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Sistema y método para proporcionar acceso autorizado a contenido digital

Antecedentes

La programación de TV de pago digital proporcionada a los descodificadores (STBs – Set Top Boxes, en inglés) de cable y satélite durante mucho tiempo ha sido proporcionada con acceso condicional y gestión de derechos digitales (DRM – Digital Rights Management, en inglés). Como se ha entendido convencionalmente, el acceso condicional se refiere al control del acceso a la transmisión o emisión particulares, independientemente del contenido específico en tal transmisión o emisión. PowerKEY, de Scientific Atlanta, y MediaCipher, de Motorola, son ejemplos comunes de tecnologías de acceso convencionales. También, como se ha entendido convencionalmente, DRM se refiere al control del acceso a un contenido particular, independientemente del modo de transmisión o emisión de tal contenido.

Un planteamiento convencional para la gestión de clave de codificación de los sistemas de DRM actuales implica el suministro de una clave de descodificación de contenido normalmente estático para cada receptor, tal como un STB de cable o satélite, por lo que la clave de descodificación de contenido está codificada con la clave pública de ese receptor y digitalmente firmada por el proveedor de servicio, tal como el servicio de TV por cable (CATV – CAble TV, en inglés) o de TV por satélite. El receptor utiliza entonces la clave de descodificación de contenido para descodificar y acceder al contenido proporcionado por el proveedor de servicio. Este planteamiento convencional proporciona un nivel inadecuado de seguridad para contenido de tipo premium porque la misma clave de descodificación de contenido estático se utiliza para una sola pieza de contenido. Así, cuando un proveedor de servicio emite ese contenido, puede ser visto por cualquiera que posea la clave de descodificación de contenido asociada con tal contenido, cuya clave puede haber sido averiguada e ilegalmente distribuida en la Internet o similar. El alcance de tal brecha de seguridad es potencialmente infinito y se termina sólo después de que es descubierta, y el contenido es recodificado con una nueva clave de descodificación de contenido.

Otro problema asociado con el planteamiento de gestión convencional de clave es que no escala suficientemente bien para soportar los sistemas de emisión. Esto es porque la codificación pública de la clave utilizada para proporcionar una clave de descodificación de contenido para cada usuario es demasiado lenta y requeriría una inversión por parte de un operador de grandes cantidades de hardware costoso. Esto es especialmente problemático para las emisiones de Pago Por Visión (PPV – Pay Per View, en inglés), donde millones de potenciales usuarios solicitarán la descodificación durante un relativamente corto periodo de tiempo.

Compendio

Por consiguiente, en esta memoria se describen realizaciones que proporcionan un planteamiento para la gestión de clave codificada para una arquitectura de gestión de derechos digitales (DRM – Digital Rights Management, en inglés) que incluye múltiples niveles de gestión de clave para minimizar el uso del ancho de banda, aun maximizando la seguridad para la arquitectura de DRM. En un ejemplo, se proporciona una estructura de datos para la gestión de clave codificada que incluye un par de claves pública / privada y tres capas adicionales de claves simétricas para autorizar el acceso a una pluralidad de contenidos.

BREVE DESCRIPCIÓN De LOS DIBUJOS

Se ilustran realizaciones a modo de ejemplo en las figuras siguientes, en las cuales números iguales indican elementos iguales, donde:

la FIG. 1 ilustra una vista de alto nivel de un sistema de distribución de contenido 100 de acuerdo con una realización;

la FIG. 2 ilustra una jerarquía de gestión de clave para una arquitectura de DRM de acuerdo con una realización;

la FIG. 3 ilustra una configuración de alto nivel para un receptor de acuerdo con una realización;

la FIG. 4 ilustra un flujo de proceso para implementar la jerarquía de gestión de clave ilustrada en la FIG. 1, de acuerdo con una realización;

la FIG. 5 ilustra un flujo de proceso detallado para la jerarquía de gestión de clave ilustrada en la FIG. 2, de acuerdo con una realización;

la FIG. 6 ilustra una jerarquía de gestión de clave alternativa para una arquitectura de DRM de acuerdo con una realización; y

la FIG. 7 ilustra un flujo de proceso detallado para la jerarquía de gestión de clave ilustrada en la FIG. 6.

Descripción Detallada

Con propósitos de sencillez e ilustrativos, los principios de las realizaciones se describen con referencia principalmente a ejemplos de los mismos. En la siguiente descripción, se explican numerosos detalles específicos para proporcionar un profundo conocimiento de las realizaciones. En otros casos, los métodos y estructuras bien conocidos no han sido descritos para no oscurecer innecesariamente las realizaciones.

La FIG. 1 ilustra una vista de alto nivel de un sistema de distribución de contenido 100 de acuerdo con una realización. El sistema 100 incluye un proveedor de servicio 110, una red de transmisión inalámbrica 120 (tal como una red de transmisión por satélite), una red de transmisión terrestre 130 (tal como una Red de Área Terrestre o una red de cable), una pluralidad de receptores 140a-140n y 150a-150n para que los usuarios reciban contenido de un proveedor de servicio 110 a través de la red de transmisión por satélite 120. Tal como se refiere en esta memoria, el contenido proporcionado a los usuarios incluye cualquier dato o información de audio o video, tal como servicios de audio transmitidos en tiempo real, servicios de video transmitidos en tiempo real, servicios de datos transmitidos en tiempo real o archivos protegidos por DRM que son emitidos utilizando un protocolo tal como FLUTE. Tal como se refiere también en esta memoria, un usuario es un individuo, un grupo de individuos, una compañía, una corporación o cualquier otra entidad que compre, suscriba o esté de otra forma autorizada para recibir acceso a uno o más contenidos particulares. Ejemplos de usuarios son, pero no están limitados a, abonados de CATV, abonados de TV por satélite, abonados de radio por satélite y compradores de Pago Por Visión (PPV – Pay Per View, en inglés) de eventos de PPV. Tal como se refiere también en esta memoria, un evento de PPV es un contenido particular para el cual se le factura a un usuario cada vez que se accede a tal contenido.

Como se hará referencia también en esta memoria, un proveedor de servicio es un individuo, un grupo de individuos, una compañía, una corporación o cualquier otra entidad que distribuya contenido a uno o más usuarios. Ejemplos de proveedores de servicio son proveedores o compañías de CATV, TV por satélite, radio por satélite y música en línea. A su vez, el proveedor de servicio recibe contenido de uno o más proveedores de contenido (no mostrados), tal como estudios cinematográficos, compañías discográficas, redes de emisión de televisión, etc. Debe observarse que un proveedor de contenido es también operable como un proveedor de servicio para proporcionar directamente su contenido a usuarios de la misma manera que se muestra para el proveedor de servicio 110 en la FIG. 1. Como se hace referencia también en esta memoria, un receptor es un dispositivo que un usuario utiliza para acceder a contenido proporcionado por un proveedor de servicio (o proveedor de contenido), a cuyo contenido tiene el usuario autorización a acceder. Ejemplos de receptores son descodificadores de CATV y de TV por satélite y receptores de radio por satélite. Debe observarse que un receptor es operable como una unidad independiente o una parte integral de un dispositivo de visión de contenido, tal como una televisión con un receptor de satélite o de CATV integrado.

La FIG. 2 ilustra una jerarquía de gestión de clave 200 para una arquitectura de DRM que es capaz de proporcionar acceso condicional y DRM de contenido a una pluralidad de usuarios. La estructura de DRM es operable como una estructura de datos legibles por ordenador codificada en un medio legible por ordenador y escalable para acomodar a los usuarios aun minimizando el uso del ancho de banda y sin la adición de caros aceleradores de hardware. La jerarquía de gestión de clave 200 es operable en un entorno de multidifusión de IP de un solo sentido, donde no hay ninguna ruta de retorno disponible desde cada receptor. No obstante, se contemplan realizaciones alternativas en las cuales la jerarquía de gestión de clave 200 está también optimizada para operación en un entorno de multidifusión de IP bidireccional, donde al menos uno o más receptores posee una capacidad de enviar mensajes de flujo de enlace ascendente sobre IP al proveedor de servicio.

En referencia a la FIG. 2, cada receptor posee un único par de claves pública / privada, donde se muestra una clave privada de dispositivo 210 del par de claves, y un certificado digital 115 correspondiente, tal como un certificado X.509, que ha sido emitido por una autoridad de certificación (CA – Certificate Authority, en inglés) para verificar que la clave pública del par de claves pública / privada pertenece al receptor particular. En un entorno de multidifusión de IP bidireccional, el receptor sube su certificado digital 115 a un proveedor de servicio durante un registro de usuario con un proveedor de servicio. En un entorno de multidifusión de IP de una sola dirección, en lugar de que un receptor suba su certificado digital durante el registro, cada CA publica sus certificados X.509 para receptores en un directorio en línea o en cualquier ubicación que sea accesible por proveedores de servicio. Debido a que los certificados digitales contienen sólo información pública, no se requiere ninguna seguridad especial para acceder a este directorio.

El único par de claves pública / privada para cada receptor es creado desde cualquier algoritmo de clave pública. Ejemplos de algoritmos de clave pública disponibles incluyen, pero no están limitados a, Rivest-Shamir-Adlerman (RSA), combinación de El-Gamal and Digital Signature Algorithm (DSA), y Curva Elíptica. En una realización, la Curva Elíptica se emplea porque su rendimiento de codificación aumenta linealmente con el tamaño de la clave. Así, la Curva Elíptica es capaz de proporcionar un adecuado nivel de seguridad con tamaños de clave más pequeños relativamente y menor complejidad.

Como se muestra en la FIG. 2, la clave de alto nivel en la jerarquía de gestión de clave 200 es el par de claves pública / privada mencionados anteriormente, como se representa mediante la clave privada del dispositivo 210.

Esta operación de clave asimétrica es elegida sobre una clave simétrica por razones de seguridad. Por ejemplo, aun teniendo una base de datos globales en línea de claves simétricas plantea un tremendo problema de seguridad y requiere precauciones de seguridad extremas, hay menores problemas de seguridad creando una base de datos en línea de certificados digitales (los certificados digitales son tratados a menudo como información pública, mientras que otra información en una base de datos de usuario, tal como habilitaciones, debe permanecer asegurada frente a un acceso no autorizado). Adicionalmente, los sistemas de clave pública proporcionan métodos estandarizados para expirar y revocar sus certificados digitales asociados.

El siguiente nivel en la jerarquía de gestión de clave 200 es una clave de unidad de dispositivo 220. Como con la clave privada de dispositivo 210, la clave de unidad de dispositivo 220 es única para cada receptor. No obstante, la clave de unidad de dispositivo 220 es simétrica, por contraposición a la asimétrica para la clave privada de dispositivo 210. En una realización, la clave de unidad de dispositivo 220 incluye múltiples claves de unidad diferentes para cada receptor, con al menos una clave para codificación y una clave para la autenticación de mensajes. Así, la clave de unidad de dispositivo 220 incluye múltiples algoritmos de codificación simétricos, que son aplicables para todos los niveles de clave simétrica en la jerarquía de gestión de clave 200. Por ejemplo, la clave de unidad de dispositivo 220 incluye una clave de acuerdo con el Estándar de Codificación Avanzada (AES – Advanced Encryption Standard, en inglés) de 128 bits utilizada para la codificación y una clave de Código de Autenticación de Mensaje con clave Hashed de 160 bits con función Hash específica (SHA-1 (HMAC SHA-1) utilizada para la autenticación del mensaje. Durante el registro de un usuario con un proveedor de servicio para servicios de contenido, el proveedor de servicio proporciona la clave de unidad de dispositivo 220 junto con las habilitaciones del dispositivo y otros datos de configuración para el receptor del usuario. La clave de unidad de dispositivo 220 es codificada con la clave pública del par de claves pública / privada antes del suministro, y es descodificada mediante la clave privada de dispositivo 210 del par de claves pública / privada cuando es recibido por el receptor.

La clave de unidad de dispositivo 220 única para cada receptor sirve para reducir el uso de ancho de banda y aumenta la escalabilidad para la seguridad del contenido. Por ejemplo, cuando se compran eventos de Pago Por Visión (PPV – Pay Per View, en inglés), las claves de programa únicas y las reglas de acceso son proporcionadas para cada receptor que solicita este evento de PPV y son así codificadas con una única clave de unidad de dispositivo 220 de cada receptor solicitante. Si no, cada clave de programa puede ser codificada y firmada digitalmente con codificación de clave pública, y el proceso se repite para cada uno de tales receptores y cada contenido de PPV solicitado allí. Un uso tan pesado de la codificación de clave pública requiere un elevado uso de ancho de banda entre el proveedor de servicio y los receptores solicitantes y provoca problemas de escalabilidad porque, potencial y severamente, limita el número de receptores que pueden ser autorizados para el mismo evento de PPV. De acuerdo con una realización, las claves de unidad de dispositivo para todos los receptores de suscripción son actualizadas con una periodicidad predeterminada, por ejemplo, una vez al año para minimizar sus posibles pirateos.

El siguiente nivel por debajo de la clave de unidad de dispositivo 220 en la jerarquía de gestión de clave 200 es una o más claves de servicio 230 para cada receptor. En una realización, las claves de servicio son utilizadas para servicios de suscripción en lugar de eventos de PPV. Cada clave de servicio 230 protege un único servicio de suscripción que es comprada como una unidad codificando el contenido de tal servicio de suscripción. Como se refiere en esta memoria, un servicio de suscripción es cualquier suscripción para contenido que es distinto de un evento de PPV. Ejemplos de un único servicio de suscripción incluyen, pero no están limitados a, un solo canal de programa físico, una porción de un canal de programa o una colección de canales de programa que son todos comprados como una unidad. Como se describirá más tarde, cada receptor periódicamente recibe un Mensaje de Gestión de Habilitación (EMM – Entitlement Management Message, en inglés) que incluye un conjunto de una o más claves de servicio, donde el EMM es codificado y autenticado con la única clave de unidad de dispositivo 220 del receptor. Se contemplan varias realizaciones donde cada EMM incluye una sola clave de servicio o múltiples claves de servicio.

Como con todas las claves simétricas de la jerarquía de gestión de clave 200, cada clave de servicio 230 incluye múltiples claves, con al menos una clave para codificación (por ejemplo, AES) y una clave para autenticación de mensaje (por ejemplo, HMAC SHA-1). De acuerdo con una realización, las claves de servicio para cada receptor son actualizadas con una periodicidad predeterminada (por ejemplo, una vez por cada periodo de tarificación) de manera que cuando un usuario cancela un servicio de suscripción, el acceso del usuario al servicio cancelado es terminado de manera codificada una vez que las claves del servicio son actualizadas.

El siguiente nivel por debajo de la clave de servicio 230 en la jerarquía de gestión de clave 200 es la clave de programa 240, que se crea para cada evento de PPV ofrecido por el proveedor de servicio, incluso si tal evento es también ofrecido a través de un servicio de suscripción. De acuerdo con una realización, cada clave de programa 240 es codificada con una única clave de unidad de servicio 220 y proporcionada a un receptor de suscripción que está asociado con la clave de unidad de dispositivo 220, junto con una o más reglas de acceso. Ejemplos de reglas de acceso incluyen restricciones geográficas (por ejemplo, bloqueo), control de contenido (que son comparadas por el receptor frente a un techo de control parental de entrada), y copian la información de control (en un caso general, esto incluye un conjunto completo de reglas de DRM que permiten que el contenido sea persistentemente

almacenado en un Grabador de Video Personal (PVR – Personal Video Recorder, en inglés), también conocido como un Grabador de Video Digital (DVR – Digital Video Recorder, en inglés), y compartida con otros dispositivos poseídos por un usuario, pero con una lista de restricciones, tal como una hora de expiración; para un contenido no persistente se desea que esta información posiblemente transmita bits de control de copia para salidas analógicas y digitales, tal como Sistema de Gestión de Guarda de Copia - Digital, o CGMS-D (de Copy Guard Management System - Digital, en inglés), y Sistema de Gestión de Guarda de Copia - Analógico, o CGMS-A (Copy Guard Management System - Analog, en inglés). Para eventos que se ofrecen sólo a través de un servicio de suscripción, sigue siendo deseable enviar reglas de acceso con una sola clave de programa 240 por programa de manera que un dispositivo de grabación pueda guardar un evento de programa individual junto con las reglas de acceso y una clave de programa 240 (en lugar de una sola clave de servicio 230 que es posiblemente utilizada para acceder a otro contenido codificado del mismo servicio de suscripción que no está autorizado para ser grabado). También, el uso de una clave de programa para autenticar las reglas de acceso proporciona una herramienta da protección frente a nueva reproducción – no es posible reproducir de nuevo las reglas de acceso de un evento de programa antiguo y hacer que pasen como las reglas de acceso para el evento actual. Debido a que la jerarquía de gestión de clave 200 soporta definiciones de una suscripción de servicio flexibles y que se superponen, es posible distribuir una misma clave de programa 240 bajo más de una clave de servicio 230.

El siguiente nivel por debajo de la clave de programa 240 en la jerarquía de gestión de clave 200 es la clave de descodificación de contenido 150. De acuerdo con una realización, la clave de programa 240 no es actualmente utilizada para descodificar directamente el contenido suscrito. Por el contrario, cada cabecera de paquete de IP de contenido incluye un valor aleatorio de una longitud predeterminada (por ejemplo, 4 bytes). Tal valor se denomina a continuación en esta memoria un “ID de Clave de Contenido” o CKID” (Content Key ID, en inglés), donde ID corresponde a identificación o identificador. La combinación de la clave de programa 240 y el CKID son introducidos en una función de Hash unidireccional, tal como HMAC SHA-1, para producir la clave de descodificación de contenido 150. Así, las claves de descodificación de contenido son utilizadas para descodificar los paquetes de IP de contenido reales del evento de programa, y cambian con relativa frecuencia, por ejemplo, una vez cada varios segundos, basándose en un cambio en el CKID. Las claves de descodificación de contenido sirven como palabras de control en los mensajes de control de habilitación (ECMs – Entitlement Control Messages, en inglés) como se describirá más adelante.

Deduciendo implícitamente cada clave de descodificación de contenido 150 de una clave de programa 240 y un CKID, la jerarquía de gestión de clave 200 permite que la clave de descodificación de contenido 150 cambie con más frecuencia e independientemente de las tasas de actualizaciones de ECM. Una motivación para tener una clave de descodificación de contenido 150, en lugar de transmitir en la clave de programa 240 para el mismo propósito, es tener un nivel de clave extra donde una clave se cambia muy frecuentemente. Este frecuente cambio permite una seguridad adicional en sistemas de DRM que utilizan microprocesadores de seguridad poco costosos para la gestión de clave pero no soportan descodificación de contenido debido, por ejemplo, a insuficiente potencia de procesamiento y a incapacidad para mantener la tasa de suministro de paquetes de contenido.

Debe entenderse que los nombres para las diferentes claves en la jerarquía de gestión de clave 200 son solamente utilizados para diferenciar esas claves una de otra describiendo las diferentes realizaciones en la presente descripción. Por lo tanto, es posible proporcionar otros nombres para las claves sin desviarse del alcance de la presente descripción. Por ejemplo, es posible nombrar la clave privada de dispositivo 110, la clave de unidad de dispositivo 120, la clave de servicio 130, etc. como primera clave, segunda clave, tercera clave y así sucesivamente.

De acuerdo con un ejemplo, la jerarquía de gestión de clave 200 está implementada como una estructura de datos legible por ordenador que está codificada de manera segura en una tarjeta inteligente para su inserción en el receptor. Debido a posibles limitaciones de procesamiento en el receptor, la tarjeta inteligente tiene que proporcionar claves de descodificación de contenido 150 a un procesador anfitrión general o a un procesador de video en el receptor que no tiene el mismo nivel de seguridad física. Sin embargo, cualquier pirateo de las claves de descodificación de contenido 150 se minimiza porque, como se ha explicado anteriormente, las claves de descodificación de contenido 150 son cambiadas frecuentemente. Este frecuente cambio fuerza a que cualquier pirateo de las claves de descodificación de contenido 150 incluya la rotura y redistribución en tiempo real de miles de claves de descodificación de contenido a una alta velocidad – haciendo tales ataques menos prácticos y más fácilmente detectables. A medida que la velocidad de cambio en las claves de descodificación de contenido aumenta, el pirateo de tales claves de descodificación de contenido resulta cada vez menos práctico.

En otro ejemplo, tal estructura de datos legible por ordenador para la jerarquía de gestión de clave 200 está codificada en un medio legible por ordenador (CRM – Computer Readable Medium, en inglés) que está asegurado en el receptor o es accesible de manera segura por parte del receptor. Las realizaciones de un CRM incluyen, pero no están limitadas a, un dispositivo electrónico, óptico, magnético u otro dispositivo de almacenamiento o de transmisión capaz de proporcionar un procesador en el receptor con instrucciones legibles por ordenador. Otros ejemplos de un CRM adecuado incluyen, pero no están limitados a, un disco flexible, un CD-ROM, un DVD, un disco magnético, un microprocesador de memoria, una ROM, una RAM, un ASIC, un procesador configurado, cualquier

medio óptico, cualquier cinta magnética o cualquier otro medio magnético, o cualquier otro medio desde el cual un procesador pueda leer instrucciones.

La FIG. 3 ilustra una configuración de alto nivel de un receptor 300 que representa cualquiera de los receptores 140a-n y 150a-n mostrados en la FIG. 1, de acuerdo con una realización. El receptor 300 incluye un procesador anfitrión 310, una memoria tal como un CRM 320, un módulo de tarjeta inteligente 330 opcional y un módulo de hardware 350 seguro. El procesador anfitrión 310 es el componente responsable de la mayoría de las funciones del receptor, y accede a la memoria 320 para que las instrucciones ejecutables lleven a cabo tales funciones. No obstante, como se ha mencionado anteriormente, el procesador anfitrión no es un dispositivo seguro y es susceptible de falsificación. En consecuencia, el procesador anfitrión 310 normalmente maneja sólo claves de vida corta, tales como las claves de descodificación de contenido y los CKIDs (los piratas informáticos están principalmente interesados en componentes de vida más larga, tales como claves privadas de dispositivo, claves de unidad de dispositivo y claves de servicio). El módulo de tarjeta inteligente 330 opcional se utiliza para recibir una tarjeta inteligente, en la cual está codificada una estructura de datos legible por ordenador para la jerarquía de gestión de clave 200, como se ha mencionado anteriormente de acuerdo con una realización, para su ejecución por parte del procesador anfitrión 310. Alternativamente, algunos o todos los datos de la tarjeta inteligente son descargados en la memoria 320 para su ejecución por parte del procesador anfitrión 310.

El módulo de hardware 350 seguro contiene un procesador de seguridad 352, un código seguro 353 y una memoria tal como un CRM 360. En una realización, el módulo de hardware 350 seguro es un dispositivo de hardware de silicio seguro, tal como un microprocesador de silicio resistente a la falsificación. La memoria 355 es responsable de almacenar de manera segura los datos de la clave de canal 124. El procesador de seguridad 351 es un procesador seguro que maneja las funciones de procesamiento para el módulo de hardware 350 seguro, tales como la ejecución de la función unidireccional (OWF – One Way Function, en inglés) 355 (por ejemplo, la función de hash HMAC-SHA-1) utilizada para producir claves de descodificación de contenido tal como se ha descrito anteriormente. El código seguro 353 es una porción del módulo de hardware 350 seguro que comprende varios códigos y aplicaciones de software que son ejecutados por el procesador de seguridad. Notablemente, un código seguro 353 incluye la OWF 355. Como se ha descrito anteriormente, es posible implementar la jerarquía de gestión de clave 200 como una estructura de datos legible por ordenador que es implementada en un CRM, tal como la memoria 360 en el módulo de hardware 350 seguro. En una realización alternativa, el par de claves pública / privada y las claves en los niveles inferiores tales como la clave de unidad de dispositivo, la clave de servicio, la clave de programa y la clave de descodificación de contenido son deducidas y almacenadas en la memoria 360.

El proceso para implementar la jerarquía de gestión de clave 200 para aprovisionar un acceso condicional y DRM de contenido a una pluralidad de usuarios se describe ahora con referencia a la FIG. 4, con otra referencia a la FIG. 3. Empezando en 410, un proveedor de servicio de contenido, tal como la programación de TV de pago digital, recibe una solicitud de contenido desde un usuario. El proveedor de servicio registra entonces al usuario de la manera habitual, por ejemplo, estableciendo la identidad del usuario, tal como nombre e información de contacto proporcionada por el usuario.

En 420, en una realización, como parte del registro, el usuario obtiene un receptor de un proveedor de servicio, por lo que al receptor se le proporciona un solo par de claves pública / privada y un certificado digital que ha sido pre-instalado, por ejemplo, en un centro de fabricación, antes de que tenga lugar cualquier registro entre el usuario y el proveedor de servicio. En esta realización, el par de claves pública / privada y el correspondiente certificado digital 115 están implementados en el receptor, guardados de manera segura en una tarjeta inteligente (para su inserción en el módulo de la tarjeta inteligente 330) o CRM (tal como la memoria 360) que es accesible para lectura por parte del receptor, como se ha mencionado anteriormente. En otra realización, el proveedor de servicio efectúa una entrega física al usuario de una tarjeta inteligente o CRM en la cual están almacenados un par de claves pública / privada y un certificado digital, de manera que se provee al receptor del usuario de un acceso a la información almacenada. En otra realización más, un proveedor de servicio proporciona el par de claves pública / privada y un certificado digital instalando remotamente en el receptor de un usuario (por ejemplo, en la memoria 360) a través de una red de datos terrestre (tal como la Internet), una red de datos inalámbrica (tal como una red celular) o una combinación de redes de datos terrestre e inalámbrica.

De acuerdo con esto, al receptor de un usuario se le provee con el par de claves pública / privada y el certificado digital antes del proceso de aprovisionamiento ilustrado en la FIG. 2, que se describe con más detalle a continuación.

En 430, también como parte del registro, el proveedor de servicio proporciona al usuario una única clave de unidad de dispositivo 220 (FIG. 2) para el receptor del usuario y opcionalmente – datos de configuración de dispositivo y habilitaciones generales que no son específicos para un servicio de acceso a contenido particular (por ejemplo, para almacenamiento en la memoria 320 ó 360). La clave unidad de dispositivo 220 es proporcionada codificada con la clave pública y descodificada dentro del receptor (para su almacenamiento en la memoria 360) con la correspondiente clave privada del único par de claves pública / privada del receptor, tal como se ha descrito anteriormente.

En 440, para proporcionar al usuario cualquier servicio de acceso a contenido, el proveedor de servicio primero transmite un mensaje de gestión de habilitación (EMM – Entitlement Management Message, en inglés) al receptor del usuario para especificar las habilitaciones del usuario al servicio de acceso a contenido. El EMM es transmitido al receptor a través de conexión terrestre, (por ejemplo, en el caso de programación de CATV) o conexión inalámbrica (por ejemplo, en el caso de TV por satélite o programación de radio). El EMM es codificado así como autenticado con la clave de unidad de dispositivo 220 única para el receptor e incluye habilitaciones de servicio para el receptor (por ejemplo, para almacenamiento en la memoria 320), y una o más claves de servicio 230 (por ejemplo, para almacenamiento en la memoria 360) para cualquier servicio de suscripción. Como se ha mencionado anteriormente, debido a que las claves de servicio 230 y las claves de unidad de dispositivo 120 cambian con el tiempo, cada EMM también incluye un identificador de clave para servir como etiqueta. De acuerdo con una realización, todos los EMMs previstos para un receptor particular son también mapeados a una única dirección de multidifusión de IP para su transmisión a tal receptor. La dirección de multidifusión de IP mapeada es separada de otras multidifusiones de IP utilizadas para enviar contenido y otros tipos de mensajes de gestión de clave. Cada EMM tiene una cabecera que incluye: a) un tipo de mensaje que le indica que es un EMM; b) un ID del dispositivo (por ejemplo, de 5 bytes o más largo) que identifica al receptor para el cual está previsto el EMM; c) un identificador de la clave de unidad de dispositivo 220 utilizada para codificar el EMM (por ejemplo, de 4 bytes) que va a ser incrementado en uno tras cada cambio de la clave de unidad de dispositivo 220; y d) un código de autenticación de mensaje (MAC – Message Authentication Code, en inglés) para verificar la integridad del mensaje, donde el MAC es una clave simétrica tal como una clave HMAC-SHA-1 truncada a 12 bytes para ahorrar ancho de banda.

En 450, el proveedor de servicio transmite a continuación un mensaje de control de habilitación (ECM – Entitlement Control Message, en inglés) al receptor del usuario para especificar claves para descodificar el contenido autorizado. Así, los ECMs son mensajes que llevan claves de programa 240 y reglas de acceso, codificadas bajo una clave de servicio 230 (para un servicio de suscripción) o una clave de unidad de dispositivo 220 (para un evento de PPV). Un nuevo ECM codificado con una clave de servicio 230 y que contiene reglas de acceso y una sola clave de programa 240 es emitido para cada evento de programa incluido en un servicio de suscripción, independientemente de si tal evento de programa está también disponible como evento de PPV.

De acuerdo con una realización, un ECM tiene varios modos de suministro / codificación diferentes. En un primer modo, cuando un ECM es proporcionado para un servicio de suscripción, es codificado y autenticado con una clave de servicio 230 y es transmitido mediante una emisión o una Multidifusión de IP. Así, todos los usuarios que están autorizados para tal servicio de suscripción son capaces de recibir y descodificar ese ECM. En un segundo modo, cuando un ECM es proporcionado para un evento de PPV, es codificado y autenticado con una clave de unidad de dispositivo 220. Cuando tal evento de PPV está también disponible en un servicio de suscripción, el ECM es también codificado y autenticado con una clave de unidad de dispositivo 220 porque el receptor para el cual está previsto el evento de PPV no está autorizado para recibir la correspondiente clave de servicio 230 para tal servicio de suscripción. Así, la jerarquía de gestión de clave 200 también soporta la capacidad de que un usuario compre derechos adicionales para un único evento, tales como “compra-mediante controles” en forma de “bajo demanda”.

En referencia de nuevo a la FIG. 4, en 460, el proveedor de servicio transmite a continuación el contenido en paquetes de datos individuales que han sido codificados con una clave simétrica. En una realización, el contenido es codificado con AES de 128-bit en modo de CBC. La codificación de contenido es preferiblemente aplicada en una capa de aplicación en un sistema del proveedor de servicio, al contrario que el uso de una seguridad de IP (IPsec) para la codificación de capa 3. Esto reduce el encabezamiento del ancho de banda que es si no impuesto por las cabeceras de IPsec y reduce también la fiabilidad del sistema de seguridad de contenido en el sistema operativo subyacente. Cada paquete de contenido individual codificado incluye una cabecera de capa de aplicación con al menos la siguiente información: un CKID, tal como se describió anteriormente, un vector de inicialización (IV – Initialization Vector, en inglés) necesario para el modo de codificación de CBC y un ID de programa (o algún otro tipo de identificador para la clave del programa 240). Un IV para AES es típicamente de 16 bytes, pero para ahorrar ancho de banda, es posible deducir la IV mediante una función de hash de un solo sentido (por ejemplo, SHA-1) a partir de un menor número de bytes, tal como 4 bytes. El ID del programa apunta a una clave de programa 240 correspondiente y habilitaciones. Como se ha mencionado anteriormente, la clave del programa 240 es combinada con el CKID para deducir la clave de codificación de contenido 150.

Como se ha descrito anteriormente, cuando una pluralidad de usuarios solicita el mismo evento de PPV, cada uno de los usuarios solicitantes recibe un ECM dirigido a la unidad (esto es, un ECM específico para el receptor de cada usuario) que contiene reglas de acceso comunes para tal evento de PPV. Así, la cantidad total de ancho de banda utilizada por todos los ECMs dirigidos a la unidad puede aumentar sustancialmente debido a múltiples duplicaciones de reglas de acceso comunes. En consecuencia, se requiere un tiempo adicional para habilitar a todos los usuarios que solicitan el mismo evento de PPV. De acuerdo con esto, en una realización, para optimizar los requisitos de los anteriormente mencionados ancho de banda y encabezamiento de tiempo, se proporcionan reglas de acceso para un evento de PPV solicitado en un ECM dirigido a un grupo, de multidifusión, para todos los usuarios solicitantes, donde el ECM dirigido a un grupo, de multidifusión, está separado de los ECMs dirigidos a una unidad. Esta

realización se describe a continuación con referencia a la FIG. 5, que ilustra un flujo del proceso para el bloque 450 de la FIG. 4.

El tipo de ECMs dirigidos a un grupo, de multidifusión que es enviado a los usuarios solicitantes depende del tipo de evento de programa solicitado por el usuario. Así, en 510, el proveedor de servicio determina si el evento de programa solicitado es ofrecido a través de un servicio de suscripción, un servicio de PPV o ambos.

En 521, si el evento de programa solicitado es ofrecido sólo a través de un servicio de suscripción, el proveedor de servicio transmite a los usuarios solicitantes (en lo que sigue en esta memoria, “abonados”) un ECM dirigido a un grupo, de multidifusión, que contiene las reglas de acceso para el evento de programa solicitado, una clave de programa 240 codificada con una clave de servicio 230 y un MAC sobre al menos la clave de programa 240 codificada y las reglas de acceso, por lo que el MAC es una clave simétrica deducida de la clave de servicio 230.

En 531, si el evento de programa solicitado es ofrecido sólo a través de un servicio de PPV, el proveedor de servicio transmite a los usuarios solicitantes (en lo que sigue en esta memoria “usuarios de PPV”) un ECM dirigido a un grupo, de multidifusión, que contiene las reglas de acceso comunes para el evento de programa solicitado, cualquier regla de acceso adicional (reglas de acceso delta) u opciones que se pueden comprar por medio del método de PPV, incluso para abonados ya registrados, y un MAC sobre al menos las reglas de acceso y cualquier regla de acceso adicional, por lo que el MAC es una clave simétrica deducida de la clave de programa 240. Debido a que el EMC dirigido a un grupo, de multidifusión, no contiene ninguna clave de programa para un servicio de PPV, en 533 el proveedor de servicio transmite además a cada uno de los usuarios de PPV un ECM dirigido a una unidad, separado, que contiene la clave de programa 240 necesaria, codificada con la correspondiente clave de unidad de dispositivo 220, por lo que el ECM dirigido a una unidad ya no contiene las reglas de acceso comunes o ninguna regla de acceso adicional, con el fin de optimizar el uso del ancho de banda y el encabezamiento de tiempo para los usuarios de PPV.

En 541, si el evento de programa solicitado es ofrecido a través de usuarios tanto de suscripción como de PPV, el proveedor de servicio transmite a todos los usuarios solicitantes, abonados y usuarios de PPV similares, un ECM dirigido a un grupo, de multidifusión, que contiene los campos necesarios para los servicios tanto de suscripción como de PPV. Así, el ECM dirigido a un grupo, de multidifusión, contiene las reglas de acceso comunes para el evento de programa solicitado, cualquier regla de acceso adicional para los usuarios de PPV, una clave de programa 240 codificada con una clave de servicio 230 para los abonados, un primer MAC sobre al menos la clave de programa 240 codificada y las reglas de acceso comunes para los abonados, y un segundo MAC sobre al menos las reglas de acceso comunes y cualquier regla adicional. El primer MAC se deriva de la clave de servicio 230 para los abonados. El segundo MAC se deriva de la clave de programa 240 para los usuarios de PPV. Por lo tanto, cada uno de los usuarios solicitantes que recibe el ECM dirigido a un grupo, de multidifusión, es capaz de verificar un MAC diferente dependiendo de si el usuario solicitante particular es un abonado o un usuario de PPV. En 543, el proveedor de servicio transmite además a cada uno de los usuarios de PPV un ECM dirigido a una unidad separado que contiene la clave del programa 240 necesaria, codificada con la correspondiente clave de unidad de dispositivo 220, por lo que los ECMs dirigidos a una unidad ya no contienen las reglas de acceso comunes o cualquier regla de acceso adicional, con el fin de optimizar el uso del ancho de banda y el encabezamiento de tiempo para los usuarios de PPV.

En otra realización, para reducir más el ancho de banda del ECM utilizado para transmitir las reglas de acceso comunes, es posible dividir o clasificar por categorías las reglas de acceso comunes en dos grupos: un primer grupo de reglas de acceso cuyo envío a los usuarios se requiere en un ECM de acceso a un grupo, de multidifusión, a una velocidad mayor (un ejemplo de tal regla de acceso incluye la tasa de contenido), y un segundo grupo de reglas de acceso que pueden ser enviadas en un ECM de acceso a un grupo, de multidifusión, a los usuarios a una velocidad menor (un ejemplo de tal regla de acceso incluye el permiso de grabación, por lo que es aceptable para un usuario grabar unos pocos segundos de un evento de programa antes de que se haya enviado una regla de acceso para prohibir cualquier otra grabación). Así, el conjunto completo de reglas de acceso comunes, incluyendo los grupos primero y segundo de reglas de acceso, puede ser enviado en un ECM dirigido a un grupo, de multidifusión, a los usuarios a una velocidad menor, y el primer grupo de reglas de acceso puede ser enviado en un ECM dirigido a un grupo, de multidifusión, adicional a una velocidad mayor.

Con el fin de facilitar la transición continua de una clave de servicio 230 a la siguiente (por ejemplo, para el mismo servicio pero con diferentes fechas de expiración), un EMM es operable para incluir la clave de servicio tanto actual como siguiente. Cuando se planifica un cambio de la siguiente clave de servicio, en algún momento predeterminado antes de que se utilice la siguiente clave de servicio el EMM es repetido con la clave de servicio tanto actual como siguiente presentes con sus correspondientes IDs de clave. Una vez que se ha realizado el cambio, la clave de servicio actual expira, y la siguiente clave de servicio pasa a ser la actual y la siguiente clave de servicio no necesita ser incluida, hasta que se desee.

El siguiente esquema aplica a los cambios de clave planificados para las claves de unidad de dispositivo 120. No obstante, este esquema no aplica a claves de programa 240. En lugar de un concepto de una clave actual o

siguiente, una clave de programa 240 simplemente corresponde a un evento de ID de PPV específico, y el receptor guarda una lista de todas las claves de programa que ha recibido para todos los eventos de PPV que no han expirado.

Debido a que no se asume que un transporte de multidifusión de IP sea fiable y que no existe garantía de una ruta de retorno, EMMS y EMCs son periódicamente retransmitidos al receptor. Para minimizar más el uso del ancho de banda del mensaje, los EMMs y ECMs pueden ser eficientemente formateados con un simple método de codificación binario, tal como MIKEY (IETF RFC 3830), que es un estándar del Grupo de Trabajo de Ingeniería de Internet (IETF – Internet Engineering Task Force, en inglés) para la gestión de una clave de la capa de aplicación que es aplicable a una multidifusión de IP. Una descripción y especificación del MIKEY completa se encuentra, por ejemplo, en MICKEY: Multimedia Internet KEYing, RFC 3830, por J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Norman, de Agosto de 2004.

De acuerdo con otra realización, los EMMs incluyen habilitaciones adicionales que proporcionan información tal como un ID de dominio, una clave de dominio y restricciones de dominio (por ejemplo, límite del número de dispositivos) con el fin de dirigir dominios personales sobre los cuales se comparte contenido en múltiples dispositivos. El protocolo de gestión de clave que proporciona seguridad al contenido sobre un dominio personal es típicamente de punto a punto bidireccional sobre IP. Así, tal protocolo no necesita utilizar la misma jerarquía de gestión de clave 200 que protege el suministro de contenido inicial.

Cada flujo de ECM correspondiente a un servicio de contenido separado, ya sea un servicio de suscripción o un evento de PPV, es mapeado a una dirección de multidifusión de IP separada, que está también separada de la dirección de contenido de IP correspondiente. Esto permite que el filtrado y la separación de los paquetes de ECM de los paquetes de contenido sean llevados a cabo de manera eficiente y que la capa de IP del receptor soporte una rápida adquisición del canal. Un ECM que contiene una clave de programa 240 codificada es formateado de la misma manera que se ha descrito anteriormente; esto es, cada clave de programa 240 simplemente corresponde a un ID de evento de PPV específico, y el receptor guarda una lista de todas las claves de programa que ha recibido y con los eventos de programa asociados que no han expirado.

De acuerdo con una realización, como una mejora adicional, los ECMs para muchos servicios pueden transmitirse en un solo flujo de IP de multidifusión de baja velocidad de fondo. Según lo permita la memoria del dispositivo, los ECMs son adquiridos previamente y almacenados para reducir más el tiempo de adquisición de canal.

La FIG. 6 ilustra un ejemplo alternativo de una jerarquía de gestión de clave 600 para una estructura de DRM que no emplea claves de programa 240. La estructura de DRM es operable como una estructura de datos legible por ordenador codificados en un medio legible por ordenador. En este ejemplo, la clave privada de dispositivo 610, el certificado digital 615 y la clave de unidad de dispositivo 620 operan como se ha descrito anteriormente para la clave privada de dispositivo 210, el certificado digital 215 y la clave de unidad de dispositivo 220, respectivamente, en la jerarquía de gestión de clave 200 (FIG. 2). No obstante, sin una clave de programa, se utilizan ahora dos claves de servicio diferentes para codificar una clave de descodificación de contenido, de manera opuesta a deducir la clave de descodificación de contenido deducida de una clave de programa y un CKID como se ha descrito anteriormente. Así, la clave de descodificación de contenido puede ser enviada en un ECM dirigido a un grupo a un receptor de usuario.

De acuerdo con esto, como se muestra en la FIG. 6, en el caso de un servicio sólo de suscripción, el proveedor de servicio primero transmite un EMM a todos los abonados, donde el EMM incluye una clave de servicio de suscripción 630 para el servicio de suscripción. El EMM incluye otra información y funciona como se ha descrito anteriormente para el EMM utilizado para la jerarquía de gestión de clave 200 de la FIG. 2. La clave de servicio 630 opera como se ha descrito anteriormente para la clave de servicio 230 de la FIG. 2. A continuación, el proveedor de servicio transmite a todos los abonados un ECM dirigido a un grupo, de multidifusión, que incluye reglas de acceso comunes y una copia de la clave de descodificación de contenido 650 codificada con la clave de servicio de suscripción 630.

En el caso de un servicio sólo de PPV, el proveedor de servicio primero transmite un EMM al receptor del usuario, donde el EMM incluye una clave de servicio de PPV 640 para el servicio de PPV. Este EMM por otra parte, incluye otra información y funciones tal como se han descrito anteriormente para el EMM utilizado para la jerarquía de gestión de clave 200 en la FIG. 2. La clave de servicio de PPV 640 opera de manera similar a la clave de servicio de suscripción 630, excepto por que la clave de servicio de PPV 640 tiene una vida útil correspondiente al evento de programa de PPV en lugar de al servicio de suscripción, y cada usuario de PPV no obtiene automáticamente la siguiente clave de servicio de PPV 640 a menos que el usuario de PPV compre otro evento de programa de PPV. A continuación, el proveedor de servicio transmite a todos los usuarios de PPV un ECM dirigido a un grupo, de multidifusión, que incluye reglas de acceso comunes y una copia de la clave de descodificación de contenido 660 codificada con la clave de servicio de PPV 640.

En el caso de un evento de programa que está disponible tanto a través de un servicio de suscripción como a través de un evento de PPV, el proveedor de servicio transmite dos EMMs diferentes, uno con la clave del servicio de

suscripción 630 para los abonados y uno con la clave de servicio de PPV 640 para los usuarios de PPV. A continuación, el proveedor de servicio transmite tanto a los abonados como a los usuarios de PPV un ECM dirigido a un grupo, de multidifusión, que incluye reglas de acceso comunes y dos copias 650 y 660 diferentes de la misma clave de descodificación de contenido (codificadas con dos claves de servicio diferentes). Así, para la optimización del ancho de banda de EMC y del encabezamiento de tiempo, se incluyen dos copias 650 y 660 codificadas de la misma clave de descodificación de contenido en el mismo ECM dirigido a un grupo, de multidifusión, para su transmisión tanto a los abonados como a los usuarios de PPV, para evitar la duplicación de reglas de acceso (los usuarios de PPV pueden tener reglas de acceso adicionales incluidas en el EMC de multidifusión, como se describe con más detalle en lo que sigue).

En referencia de nuevo a la FIG. 3, como con la jerarquía de gestión de clave 200 (FIG. 2), es posible implementar la jerarquía de gestión de clave 600 como una estructura de datos legible por ordenador que es implementada en uno o más CRMs, tal como la memoria 360 en el módulo de hardware 350 seguro. De nuevo, esto asegura la seguridad de las diferentes claves de codificación / descodificación dentro del módulo de hardware 350 seguro. En una realización alternativa, el par de claves pública / privada y el certificado digital asociado están almacenados en la tarjeta inteligente, y claves en los niveles más bajos tales como la clave de unidad de dispositivo, las dos claves diferentes y la clave de descodificación de contenido son deducidas y almacenadas en la memoria 360.

La FIG. 7 ilustra un flujo de proceso para el suministro de ECMs dirigidos a un grupo, de multidifusión, sin claves de programa a usuarios basándose en el tipo de evento de programa solicitado por los usuarios. En 710, se determina si el evento de programa solicitado se ofrece a través de un servicio de suscripción, un servicio de PPV o los dos. En 721, si el evento de programa solicitado se ofrece a través de un servicio sólo de suscripción, el proveedor de servicio transmite a los abonados un ECM dirigido a un grupo, de multidifusión, que contiene las reglas de acceso comunes para el evento de programa solicitado, una primera copia 650 de la clave de descodificación de contenido codificada con una clave de servicio de suscripción 630 y un MAC sobre al menos la clave de descodificación de contenido de suscripción 650 y las reglas de acceso, por lo que el MAC es una clave simétrica deducida de la clave de servicio de suscripción 630.

En 731, si el evento de programa solicitado se ofrece a través de un servicio sólo de PPV, el proveedor de servicio transmite a los usuarios de PPV solicitantes un ECM dirigido a un grupo, de multidifusión, que contiene las reglas de acceso comunes para el evento de programa solicitado, cualquier regla de acceso adicional (reglas de acceso delta) u opciones que los usuarios solicitantes pueden comprar, incluso si son ya usuarios de PPV, una segunda copia 660 de la misma clave de descodificación de contenido codificada con una clave de servicio de PPV 640 y un MAC sobre al menos las reglas de acceso y cualquier regla de acceso adicional, por lo que el MAC es una clave simétrica deducida de la clave de servicio de PPV 640.

En 741, si el evento de programa solicitado se ofrece tanto a través de un servicio de suscripción como a través de un evento de PPV, el proveedor de servicio transmite a todos los usuarios solicitantes, abonados y usuarios de PPV similares, un ECM dirigido a un grupo, de multidifusión, que contiene los campos necesarios para los servicios tanto de suscripción como de PPV. Así, el ECM dirigido a un grupo, de multidifusión, contiene las reglas de acceso comunes para el evento de programa solicitado, cualquier regla de acceso adicional, como se ha descrito anteriormente para los usuarios de PPV, primera y segunda copias 650 y 660 codificadas de la misma clave de descodificación de contenido, un primer MAC sobre al menos las reglas de acceso comunes y la primera copia 650 codificada de la clave de descodificación de contenido para los abonados, y un segundo MAC sobre al menos las reglas de acceso comunes, cualquier regla de acceso adicional y la segunda copia 660 codificada de la misma clave de descodificación de contenido para los usuarios de PPV. El primer MAC es una clave simétrica deducida a partir de la clave de servicio de suscripción 630 y el segundo MAC es una clave simétrica deducida a partir de la clave de servicio de suscripción 640. En consecuencia, cada uno de los usuarios solicitantes que reciben el ECM dirigido a un grupo, de multidifusión es capaz de verificar un MAC diferente dependiendo de si el usuario solicitante particular es un abonado o un usuario de PPV. Los abonados y los usuarios de PPV también utilizan sus propias claves de servicio 630 y 640, respectivamente, para descodificar la copia apropiada de la clave de descodificación de contenido codificada.

De acuerdo con una realización, las jerarquías de gestión de clave ilustradas en las FIGs. 2 y 6 son operables para proporcionar acceso a contenido a receptores móviles itinerantes. En el caso de una multidifusión a móviles, itinerante se refiere a un usuario que transporta un receptor móvil fuera de un área de servicio predefinida y lo introduce en un área diferente (“área de itinerancia”) donde el usuario no puede recibir servicios de emisión (suscripción o PPV) de un proveedor de servicio con el cual el usuario se suscribe, pero donde existe un proveedor de servicio local alternativo. Así, el receptor móvil visitante es temporalmente aprovisionado para recibir emisión en el área de itinerancia desde el proveedor de servicio local. La itinerancia también se refiere a un usuario que entra en un área (“área de itinerancia”) donde el usuario no está aprovisionado para recibir servicios de emisión (suscripción o PPV) y no puede recibir y descodificar ECMs de manera automática, incluso aunque el usuario esté realmente autorizado para servicios en el área de itinerancia (por ejemplo, el área de itinerancia es cubierta por una red diferente que es operada por el mismo proveedor de servicio). Cuando el usuario está en un área de itinerancia, el usuario puede contactar con el proveedor de servicio local, que da servicio al área de itinerancia con el fin de

recibir habilitaciones temporalmente. Esto puede ser realizado interactivamente si el receptor móvil del usuario tiene una capacidad de comunicación bidireccional. Alternativamente, el usuario puede contactar con el proveedor de servicio local por teléfono.

Una vez que el usuario es verificado y autorizado por el proveedor de servicio local en el área de itinerancia para recibir servicios en ella, el proveedor de servicio local transmite al receptor del usuario un EMM con una clave de unidad de dispositivo itinerante para servicios en itinerancia que está codificada con la clave pública del par de claves pública / privada del receptor como se ha descrito anteriormente. Como se ha mencionado anteriormente, es posible que el proveedor de servicio local localice un correspondiente certificado digital para la clave pública / privada del receptor (basándose en el ID del dispositivo del receptor) de un directorio de certificados accesible globalmente. En consecuencia, el usuario es capaz de recibir EMMs y ECMs para servicios de itinerancia con el receptor del usuario como si el usuario fuese un abonado regular, excepto porque el receptor debe recibir claves de servicio a corto plazo (por ejemplo, buenas sólo para un día) en el EMM para servicios de suscripción en itinerancia. De acuerdo con esto, para dar soporte a receptores en itinerancia, el proveedor de servicio local genera dos conjuntos de ECMs separados: a) un conjunto normal de ECMs que tienen claves de programa codificadas con claves de servicio regulares para usuarios regulares con servicios de suscripción en el área, y b) un conjunto separado de ECMs de itinerancia que tienen claves de programa codificadas con las claves de servicio a corto plazo mencionadas anteriormente para usuarios en itinerancia con servicios de suscripción en el área. Además, un usuario en itinerancia es capaz de solicitar o comprar un evento de PPV, por lo que el receptor del usuario va a recibir ECMs que tienen claves de programa que están codificadas con la clave de unidad de dispositivo en itinerancia del receptor en lugar de las claves de unidad a largo plazo. La optimización del ancho de banda del ECM y los encabezamientos de tiempo como se han descrito anteriormente son aplicables también aquí.

Debido a que no se hace ninguna asunción con respecto a la seguridad de la red de IP del proveedor de servicio que se utiliza para comunicarse entre varios receptores de red implicados en la generación y el transporte de EMMs y ECMs, es posible que tales mensajes se sometan a una grabación o captura no autorizadas dentro de tal red de IP. EMMs previamente transmitidos y capturados pueden utilizarse entonces para crear significativos problemas de negación de servicio a un usuario, sobre todo cuando la clave del servicio 230 y la clave de unidad de dispositivo 220 del receptor del usuario no se cambian frecuentemente (por ejemplo, una vez al mes para la clave de servicio 230 y una vez al año para la clave de unidad de dispositivo 220). Cuando un EMM previamente capturado es reinsertado más tarde en un flujo de emisión de IP, tal como un flujo de multidifusión de IP utilizado para la transmisión del EMM, el receptor es reiniciado con una clave de unidad de dispositivo 220 antigua y obsoleta o una clave de servicio 230 que desactiva la capacidad del receptor para recibir y descodificar correctamente subsiguientes mensajes de gestión de clave. Así, de acuerdo con una realización, la protección de nueva reproducción para los EMMs es proporcionada aumentando secuencialmente los identificadores de clave para la clave de unidad de dispositivo 220 y utilizando el MAC para proporcionar integridad de mensaje. Por ejemplo, cuando un receptor detecta que un EMM particular contiene un identificador de clave que es menor que el último recibido, tal EMM es borrado e ignorado como un potencial ataque de nueva reproducción. Un emisor legitimado de EMMs nunca disminuye un identificador de clave que está codificado bajo la misma clave de unidad de dispositivo 220.

Como se ha descrito anteriormente, la clave de unidad de dispositivo 220 y la clave de servicio 230 no se cambian frecuentemente. Así, un identificador de clave de 4 bytes no va a volver a 0 en miles de años, y no es preciso preocuparse de lo que ocurra cuando un identificador de clave vuelva a 0. No obstante, para evitar cualquier error accidental cuando un identificador de clave se establezca por alguna razón en FFFF, es posible programar un receptor para verificar que el nuevo identificador de clave no ha saltado desde el valor previo en más de una cantidad razonable (por ejemplo, 100).

De acuerdo con una realización, es posible que un proveedor de servicio aproveche la jerarquía de gestión de clave 200 para una mayor escalabilidad ofreciendo a los usuarios un modelo de compra de contenido llamado almacenar y transmitir PPV o Impulsar PPV (IPPV), donde todos los receptores participantes están suficientemente seguros físicamente de que están asegurados con una clave de programa, incluso antes de que ningún contenido en ese servicio de PPV haya sido comprado. A cada receptor se le encomienda entonces la tarea de grabar localmente en el receptor qué programas de IPPV elige ver realmente un usuario y periódicamente reportar estas compras al sistema de tarificación del proveedor de servicio, el cual factura al usuario de manera correspondiente. Este modelo de IPPV es aplicable para receptores con una ruta de retorno.

Así, con la jerarquía de gestión de clave 200, la IPPV es fácilmente habilitada para permitir que todos los usuarios se suscriban a servicios de IPPV de manera gratuita. Al mismo tiempo, cualquier compra local de eventos de programa o de servicio realizada en un servicio de IPPV es grabada en el receptor, y el conjunto acumulativo de compras es entonces reportado de nuevo hacia el proveedor de servicio. Por supuesto, resulta deseable un protocolo seguro de punto a punto, bidireccional, entre cada receptor y el sistema anfitrión del proveedor de usuario para que este último solicite a cada receptor una lista de compras de IPPV que hayan sido realizadas dentro de un periodo de tiempo pasado predeterminado, por ejemplo, el último periodo de facturación. También, es posible codificar a un receptor para un programa con el fin de imponer un límite en un número de compras de IPPV que pueden ser realizadas o

una cantidad de “dinero gastado” global total hasta que el receptor reporta la lista completa de compras al proveedor de usuario. Para dar soporte a los receptores de servicio de IPPV que no necesariamente tienen una capacidad de ruta de retorno, es posible que los usuarios asociados con esos receptores pre-compren crédito en un kiosco. Una vez que el crédito se ha utilizado, un usuario puede volver a un kiosco, para reportar las compras y adquirir más crédito.

De acuerdo con un ejemplo, las jerarquías de gestión de clave 200 y 600 son operables para soportar vistas previas gratuitas para programas de PPV. En tal realización, el proveedor de servicio transmite una clave de programa de vista previa gratuita para cada receptor del usuario en un EMM poco después del registro. La distribución de claves de programa de vista previa gratuita se basa en uno o más criterios de autorización, tal como la edad o la ubicación geográfica. Cuando tiene lugar una vista previa gratuita, el proveedor de servicio transmite paquetes de datos de contenido para vista previa gratuita a los usuarios en un canal correspondiente (dirección de multidifusión de IP). Cada paquete de contenido para vista previa gratuita incluye una cabecera de capa de aplicación que tiene al menos un ID de programa de vista previa gratuita (o algún otro tipo de identificador para la clave de programa de vista previa gratuita (o algún otro tipo de identificador para la clave de programa de vista previa gratuita). Así, todos los receptores autorizados para vistas previas gratuitas son capaces de descodificar los paquetes de contenido para vista previa gratuita con una clave deducida de la clave de programa para vista previa gratuita, la cual está identificada por el ID del programa para vista previa gratuita en las cabeceras de paquete. Una vez que la vista previa gratuita finaliza, el proveedor de servicio puede transmitir paquetes de contenido que no son para vista previa gratuita, con el fin de indicar un ID de programa diferente, el cual requiere a continuación una clave de programa que se obtiene a través de una suscripción PPV o compra de IPPV, basándose en los mecanismos descritos anteriormente.

De acuerdo con otra realización, si las reglas de acceso al programa están autorizadas para incluir restricciones de servicios de tiempo seguras o autenticadas, tales como “el contenido puede ser grabado en un PVR y utilizado localmente durante un periodo de tiempo limitado”, es posible que el receptor asegure una fuente de tiempo de manera que el contenido temporalmente almacenado se programe para expirar de manera segura. Para alcanzar este esquema, se envían repetidamente mensajes de tiempo o paquetes a una dirección de multidifusión de IP específica para el receptor que tiene la capacidad de almacenar persistentemente la programación de contenido, tal como PVR o DVR. Cada mensaje de tiempo incluye una marca de fecha de una determinada longitud (por ejemplo, 4 bytes) en hora UTC, un número secuencial y una firma digital tal como un RSA o ECDSA.

El receptor es entonces aprovisionado (por ejemplo, en un Mensaje de EMM) tanto con el número secuencial actual como con una cadena de certificado del servidor de tiempo con el fin de validad cada mensaje de tiempo. Un número secuencial en un mensaje de tiempo debe ser mayor o igual que el de un mensaje de tiempo previo. En casos en los que el número secuencial es el mismo, la marca de tiempo más nueva debe ser mayor o igual a la última recibida. Así, este número secuencial es operable para realizar ajustes de tiempo hacia atrás según se desee o requiera. Siempre que las marcas de tiempo se estén incrementando estrictamente, no hay necesidad de cambiar nunca este número secuencial.

Si un número significativo de receptores tienen acceso a una ruta de retorno, entonces pueden lograrse mejoras adicionales en la escalabilidad y los tiempos de adquisición de contenido. Siempre que la capacidad bidireccional de cada receptor sea conocida para el proveedor de servicio, los flujos de EMMs y de ECMs dirigidos a una unidad que se repiten periódicamente no necesitan incluir ningún mensaje dirigido a esos receptores bidireccionales. Un receptor con una capacidad bidireccional es operable para enviar un mensaje hacia arriba para solicitar su EMM o ECM dirigido a una unidad y esperar que la respuesta vuelva. Si la respuesta no vuelve debido a un transporte no fiable, el receptor es operable para reintentarlo después de que transcurra un periodo de tiempo predeterminado. Siempre que el proveedor de servicio no vea una solicitud explícita de un receptor bidireccional, el proveedor de servicio no necesita multidifundir ningún mensaje que esté específicamente codificado para ese dispositivo.

REIVINDICACIONES

1. Un método llevado a cabo por un proveedor de servicio para proporcionar un acceso autorizado a un contenido de PPV, que comprende las etapas de:

recibir una solicitud de acceso a un contenido desde una pluralidad de usuarios;

en respuesta a la solicitud de acceso, proporcionar un par de claves asimétricas que tienen una clave de codificación pública y una clave de codificación privada para cada uno de la pluralidad de usuarios;

proporcionar una única clave de unidad de dispositivo para cada uno de la pluralidad de usuarios, donde cada una de las claves de unidad de dispositivo está codificada con la clave de codificación pública asociada con cada usuario;

proporcionar un primer mensaje de control de habilitación (ECM – Entitlement Control Message, en inglés) para la solicitud de acceso, incluyendo la etapa de proporcionar el primer ECM:

a) proporcionar reglas de acceso para la solicitud de acceso en el primer ECM;

b) proporcionar un primer código de autenticación de mensaje (MAC – Message Authentication Code, en inglés) para al menos las reglas de acceso en el primer ECM; y

c) proporcionar el primer ECM como un ECM dirigido a un grupo, de multidifusión a la pluralidad de usuarios; y además,

proporcionar un segundo ECM para la solicitud de acceso, donde la etapa de proporcionar el segundo ECM incluye:

a) codificar una primera copia de una clave de programa con la clave de unidad de dispositivo, siendo la clave de programa operable para descodificar el contenido para la solicitud de acceso y deducir el primer MAC; y

b) proporcionar la primera copia codificada de la clave de programa en el segundo ECM; y

donde proporcionar el segundo ECM comprende proporcionar el segundo ECM como un ECM dirigido a una unidad para cada uno de la pluralidad de usuarios, donde el ECM dirigido a una unidad incluye una clave de programa codificada con la clave de unidad de dispositivo que es única para cada uno de los usuarios.

2. El método de la reivindicación 1, que comprende también las etapas de:

recibir una solicitud de acceso a otro servicio para el contenido; y

en respuesta a la solicitud de acceso al otro servicio, proporcionar un mensaje de gestión de habilitación (EMM – Entitlement Management Message, en inglés), incluyendo la etapa de proporcionar el EMM,

a) codificar una clave de servicio con una clave de unidad de dispositivo que es única para una fuente de la otra solicitud de acceso a servicio, siendo la clave de servicio operable para proporcionar la codificación y descodificación de la clave de programa; y

b) proporcionar la clave de servicio codificada en el EMM.

3. El método de la reivindicación 3, en el que en repuesta a la solicitud de acceso al otro servicio, la etapa de proporcionar el primer ECM incluye también:

c) proporcionar reglas de acceso a otro servicio para el acceso a otro servicio en el primer ECM;

d) codificar una segunda copia de la clave de programa con la clave de servicio;

e) proporcionar la segunda copia de la clave de programa en el primer ECM; y

f) proporcionar un segundo MAC para al menos las reglas de acceso a otro servicio y la segunda copia de la clave de programa, siendo la segunda copia de la clave de programa operable para descodificar el contenido para el acceso al otro servicio y deducir el segundo MAC.

4. El método de la reivindicación 1, en el que la etapa de proporcionar reglas de acceso para la solicitud de acceso en el primer ECM comprende las etapas de:

proporcionar un subconjunto predeterminado de las reglas de acceso para la solicitud de acceso en el primer ECM y una primera velocidad; y

proporcionar un recordatorio de las reglas de acceso en el primer ECM a una velocidad menor que la velocidad de proporcionar el subconjunto predeterminado de reglas de acceso, donde el recordatorio de las reglas de acceso en el primer ECM comprende todas las reglas del primer ECM que no forman parte del subconjunto predeterminado.

5. El método de la reivindicación 1, que comprende también las etapas de:

recibir una solicitud de itinerancia para el contenido, donde la solicitud de itinerancia es una solicitud de acceso a itinerancia o una solicitud de acceso a otro servicio; y

en respuesta a la solicitud de itinerancia, proporcionar una clave de unidad de dispositivo de itinerancia que es única para una fuente de la solicitud de itinerancia.

6. El método de la reivindicación 5, que comprende también la etapa de:

en respuesta a la solicitud de itinerancia que es la solicitud de acceso de itinerancia, proporcionar un ECM de itinerancia, incluyendo la etapa de proporcionar el ECM de itinerancia,

a) codificar una clave de programa de itinerancia con la clave de unidad de dispositivo de itinerancia, siendo la clave de programa de itinerancia operable para descodificar el contenido para la solicitud de acceso mediante itinerancia; y

b) proporcionar la clave de programa de itinerancia en el ECM de itinerancia.

7. El método de la reivindicación 5, que comprende también la etapa de:

en repuesta a la solicitud de itinerancia que es la solicitud de acceso a otro servicio, proporcionar un EMM de itinerancia, donde la etapa de proporcionar el EMM incluye,

c) codificar una clave de servicio de itinerancia con al menos la clave de unidad de dispositivo de itinerancia; y

d) proporcionar la clave de servicio de itinerancia en el EMM de itinerancia.

8. El método de la reivindicación 7, que comprende también la etapa de:

en respuesta a que la solicitud de itinerancia es la solicitud de acceso a otro servicio, proporcionar un ECM de itinerancia, incluyendo la etapa de proporcionar el ECM de itinerancia,

a) codificar una clave de programa de itinerancia con la clave de servicio de itinerancia, siendo la clave de programa de itinerancia operable para descodificar el contenido para el acceso al otro servicio mediante itinerancia; y

b) proporcionar la clave de programa de itinerancia en el ECM de itinerancia.

9. El método de la reivindicación 1, que comprende también la etapa de:

proporcionar un mensaje de gestión de habilitación (EMM – Entitlement Management Message, en inglés) que incluye una clave de programa de vista previa gratuita, donde la clave del programa para vista previa gratuita es operable para permitir una vista previa gratuita de contenido mediante la solicitud de acceso.

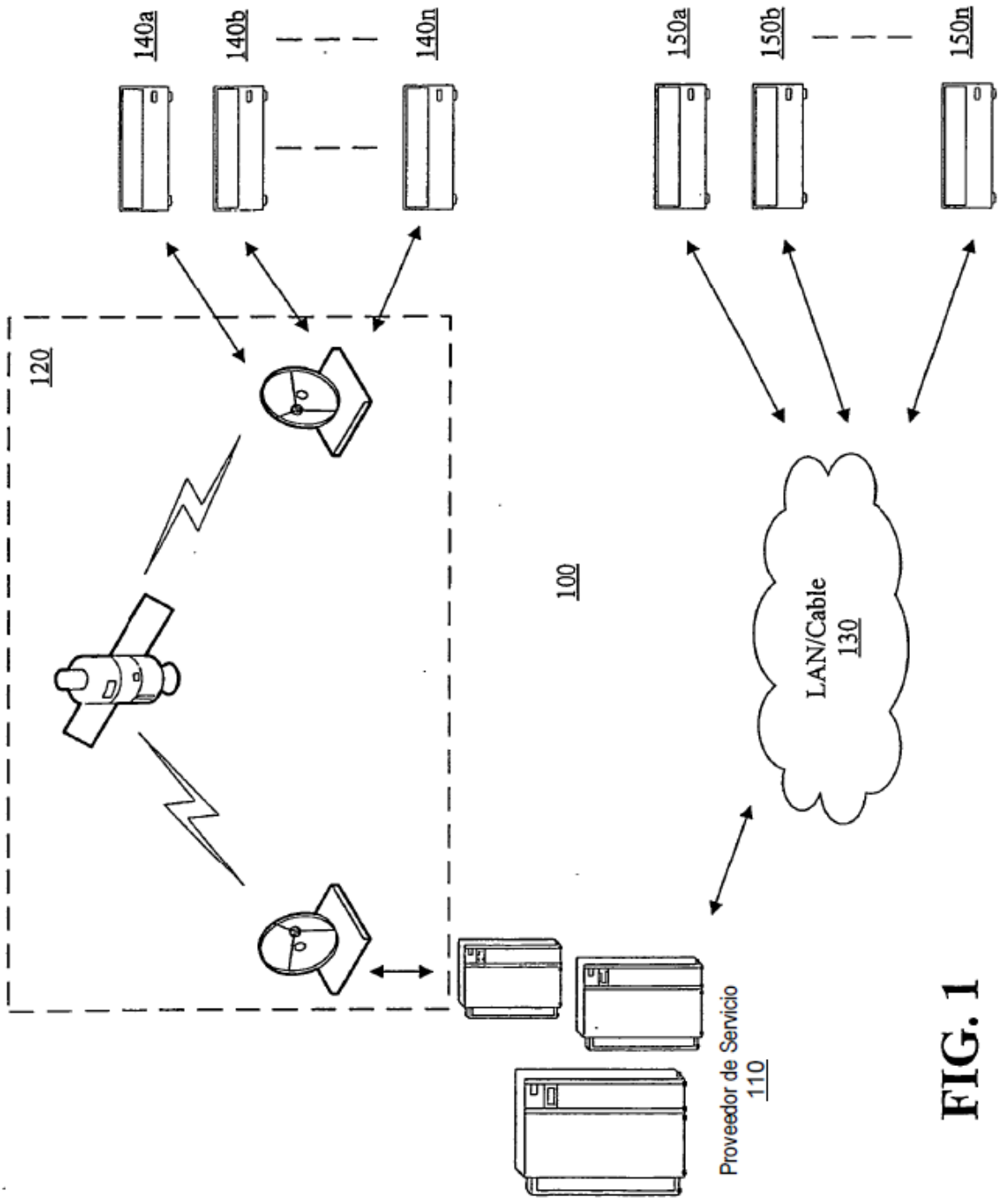
140a
140b
140n
150a
150b
150n
120
100
LAN/Cable
130
Proveedor de Servicio
110

FIG. 1

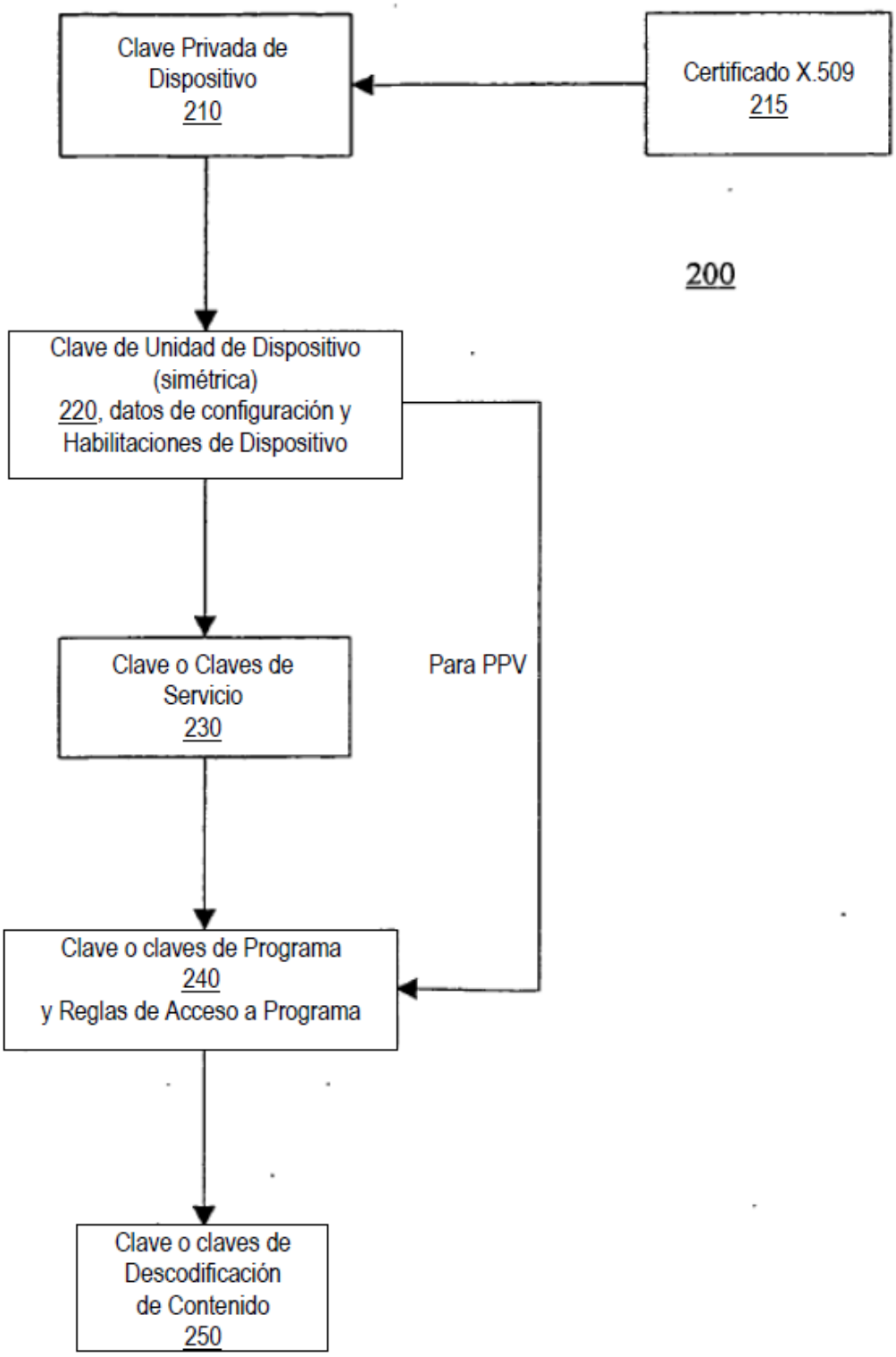
Clave Privada de Dispositivo
210
Certificado X.509
215
200
Clave de Unidad de Dispositivo (simétrica)
220, datos de configuración y Habilitaciones de Dispositivo
Clave o Claves de Servicio
230
Para PPV
Clave o claves de Programa
240
y Reglas de Acceso a Programa
Clave o claves de Descodificación de Contenido
250

FIG. 2

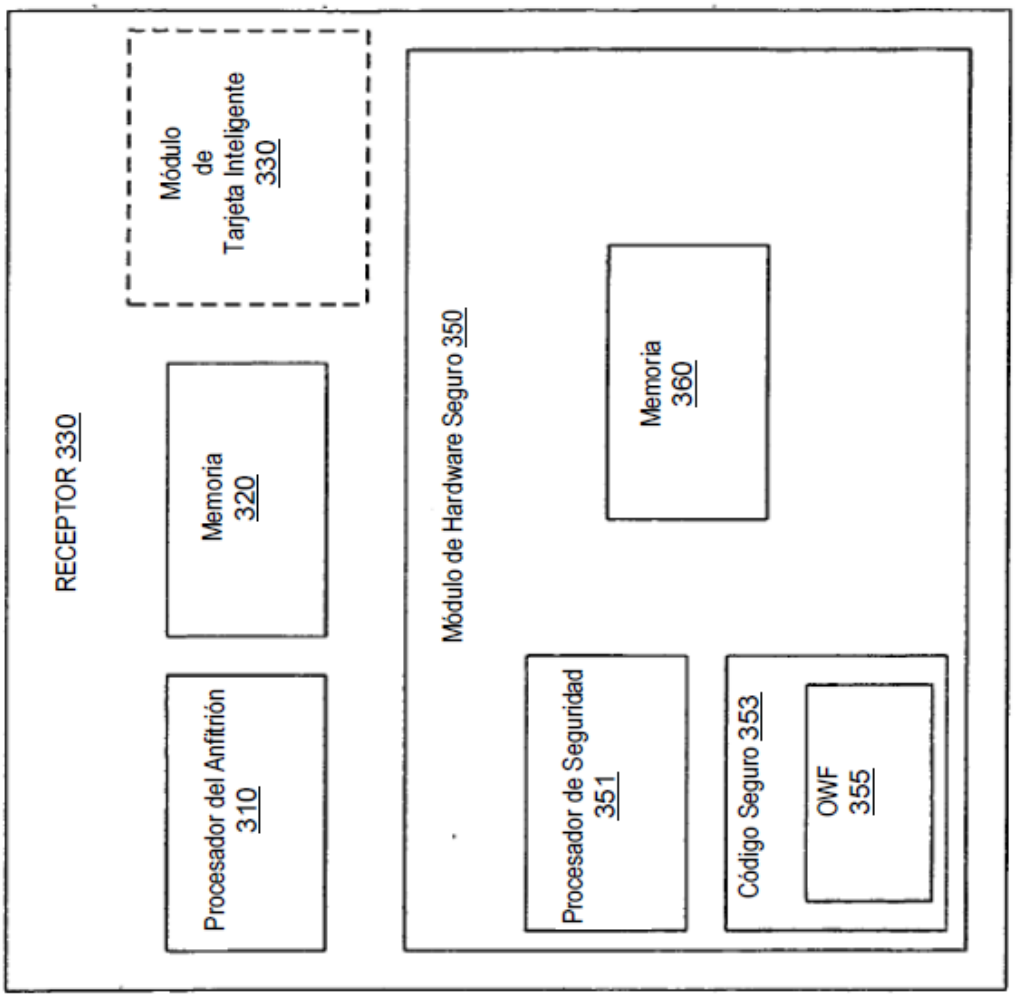
RECEPTOR 330
Módulo de Tarjeta Inteligente 330
Memoria 320
Procesador del Anfitrión 310
Módulo de Hardware Seguro 350
Memoria 360
Procesador de Seguridad 351
Código Seguro 353
OWF 355

FIG. 3

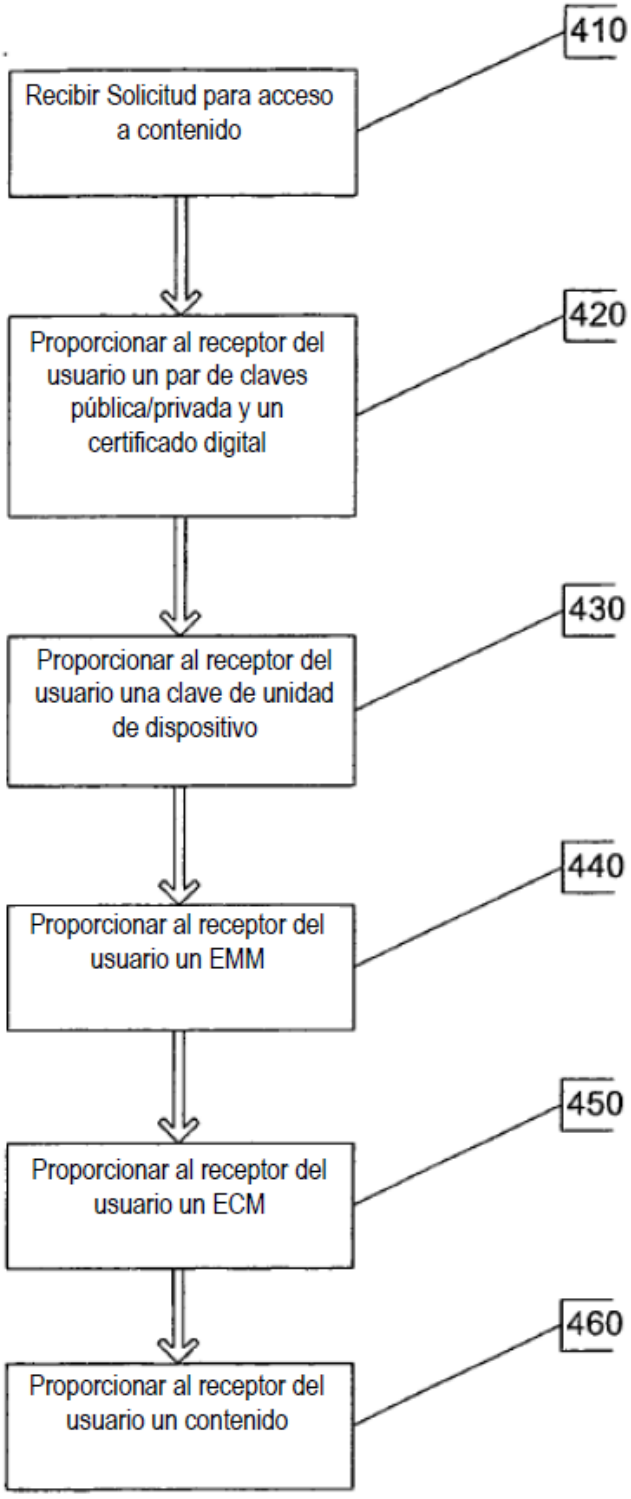
410
Recibir Solicitud para acceso a contenido
420
Proporcionar al receptor del usuario un par de claves pública/privada y un certificado digital
430
Proporcionar al receptor del usuario una clave de unidad de dispositivo
440
Proporcionar al receptor del usuario un EMM
450
Proporcionar al receptor del usuario un ECM
460
Proporcionar al receptor del usuario un contenido

FIG. 4

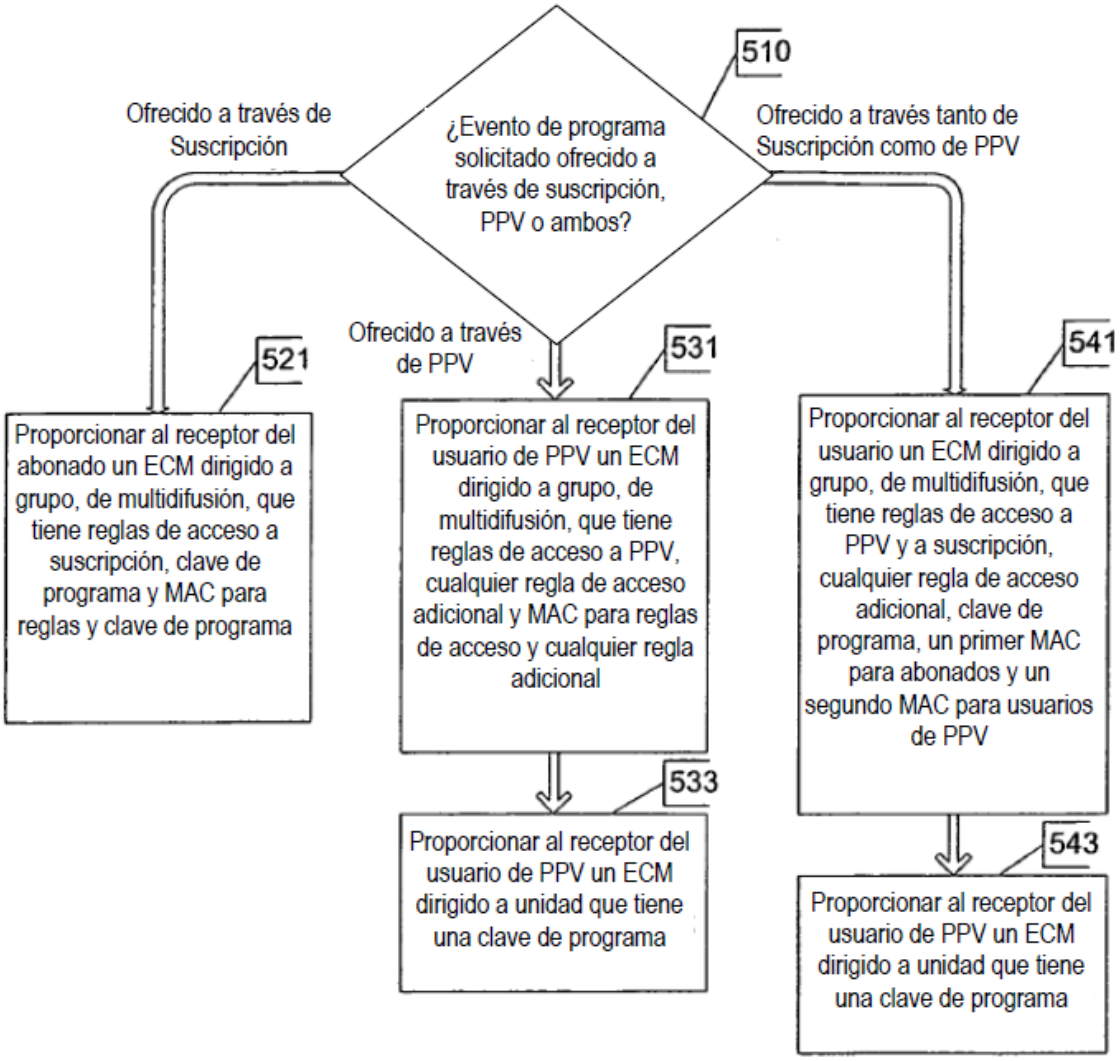
510
¿Evento de programa solicitado ofrecido a través de suscripción, PPV o ambos?
Ofrecido a través de Suscripción
Ofrecido a través de PPV
Ofrecido a través tanto de Suscripción como de PPV
521
Proporcionar al receptor del abonado un ECM dirigido a grupo, de multidifusión, que tiene reglas de acceso a suscripción, clave de programa y MAC para reglas y clave de programa
531
Proporcionar al receptor del usuario de PPV un ECM dirigido a grupo, de multidifusión, que tiene reglas de acceso a PPV, cualquier regla de acceso adicional y MAC para reglas de acceso y cualquier regla adicional
533
Proporcionar al receptor del usuario de PPV un ECM dirigido a unidad que tiene una clave de programa
541
Proporcionar al receptor del usuario un ECM dirigido a grupo, de multidifusión, que tiene reglas de acceso a PPV y a suscripción, cualquier regla de acceso adicional, clave de programa, un primer MAC para abonados y un segundo MAC para usuarios de PPV
543
Proporcionar al receptor del usuario de PPV un ECM dirigido a unidad que tiene una clave de programa

FIG. 5

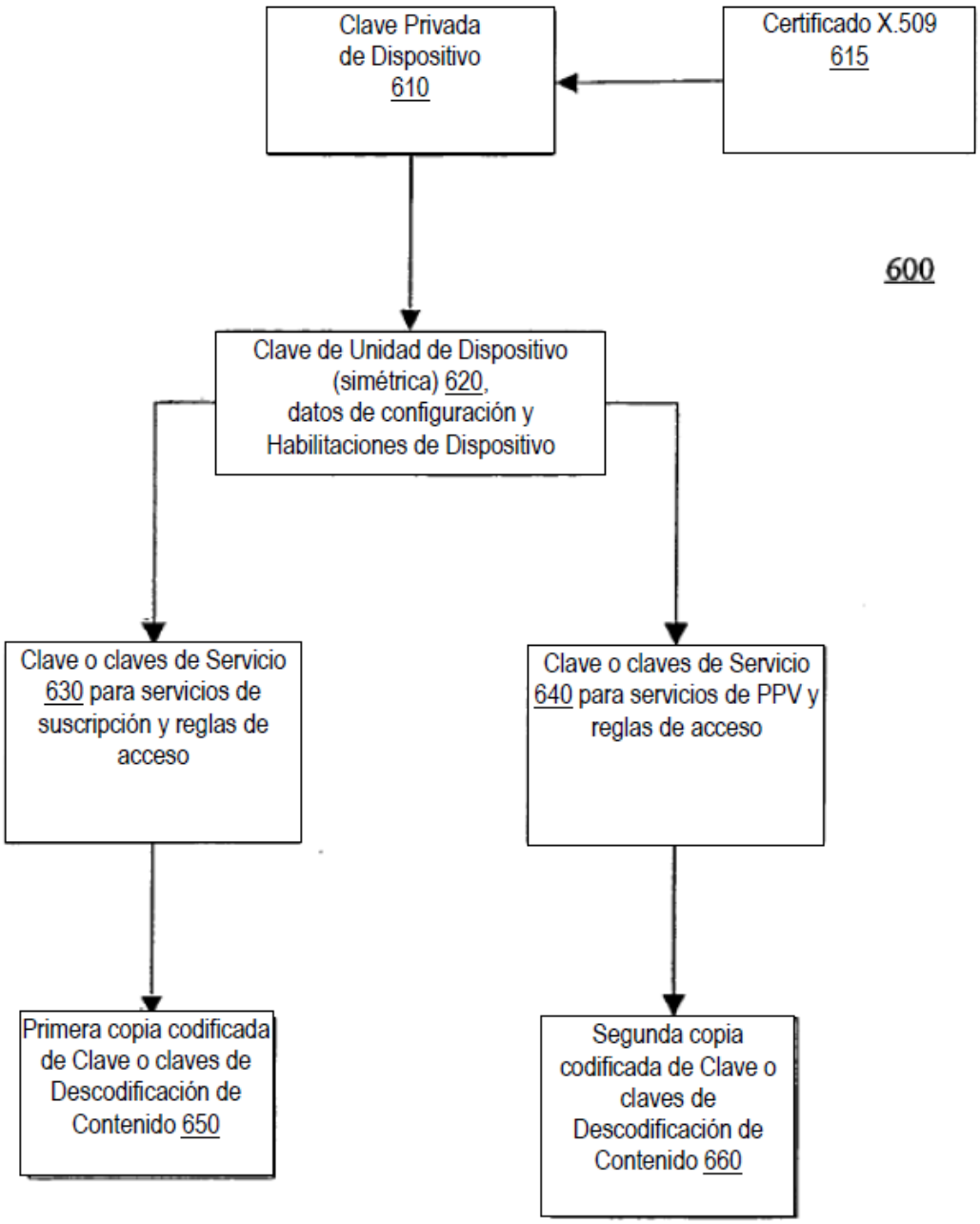
Clave Privada de Dispositivo 610
Certificado X.509 615
600
Clave de Unidad de Dispositivo (simétrica) 620, datos de configuración y Habilitaciones de Dispositivo
Clave o claves de Servicio 630 para servicios de suscripción y reglas de acceso
Clave o claves de Servicio 640 para servicios de PPV y reglas de acceso
Primera copia codificada de Clave o claves de Descodificación de Contenido 650
Segunda copia codificada de Clave o claves de Descodificación de Contenido 660

FIG. 6

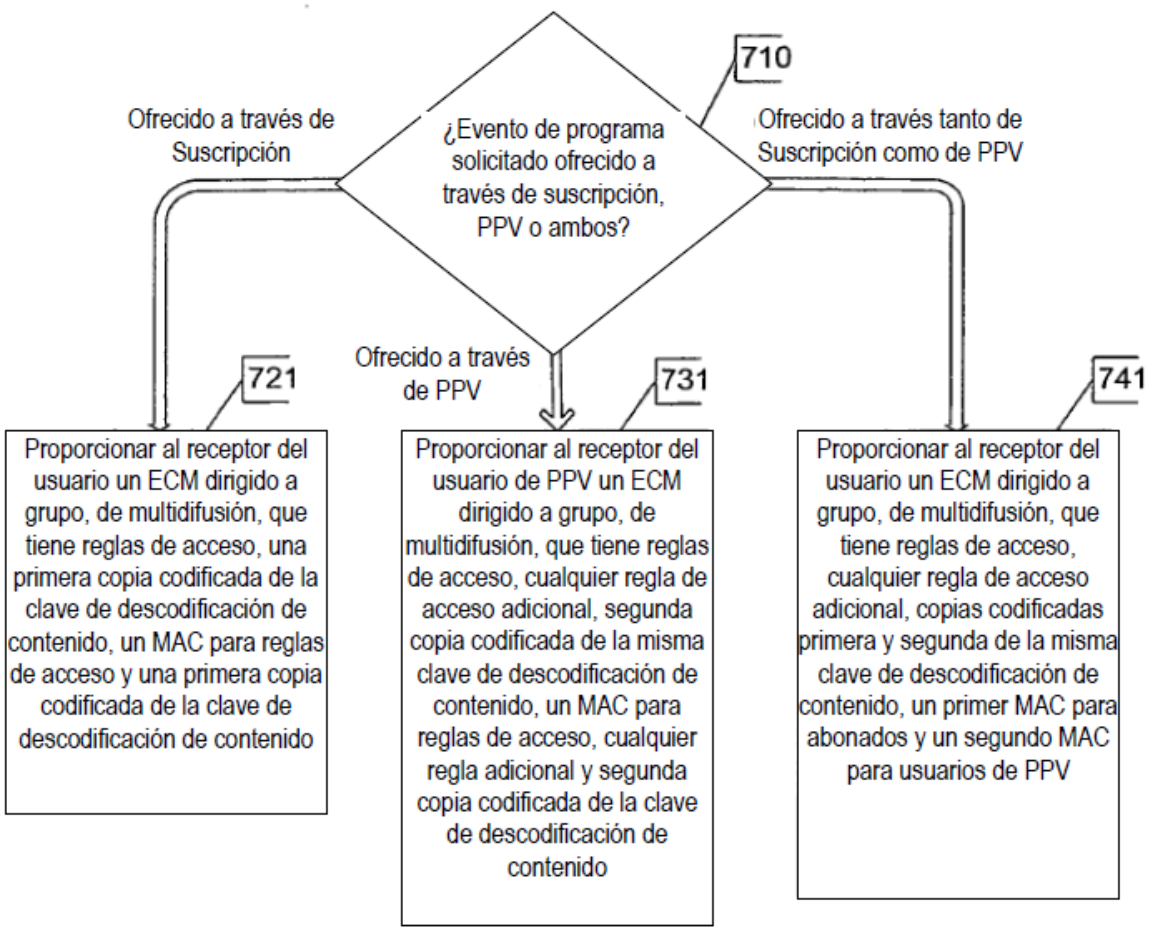
710
¿Evento de programa solicitado ofrecido a través de suscripción, PPV o ambos?
Ofrecido a través de Suscripción
Ofrecido a través de PPV
Ofrecido a través tanto de Suscripción como de PPV
721
731
741
Proporcionar al receptor del usuario un ECM dirigido a grupo, de multidifusión, que tiene reglas de acceso, una primera copia codificada de la clave de descodificación de contenido, un MAC para reglas de acceso y una primera copia codificada de la clave de descodificación de contenido
Proporcionar al receptor del usuario de PPV un ECM dirigido a grupo, de multidifusión, que tiene reglas de acceso, cualquier regla de acceso adicional, segunda copia codificada de la misma clave de descodificación de contenido, un MAC para reglas de acceso, cualquier regla adicional y segunda copia codificada de la clave de descodificación de contenido
Proporcionar al receptor del usuario un ECM dirigido a grupo, de multidifusión, que tiene reglas de acceso, cualquier regla de acceso adicional, copias codificadas primera y segunda de la misma clave de descodificación de contenido, un primer MAC para abonados y un segundo MAC para usuarios de PPV

FIG. 7